

**IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF MISSOURI**

IN THE MATTER OF THE SEARCH OF:

**DROPBOX, INC. ACCOUNT WITH THE
SCREEN / USER NAME: Sam Smith,
Dropbox ID: 2703411392, and the email
address of sstevie625@gmail.com THAT IS
STORES AT PREMISES CONTROLLED
BY DROPBOX, INC.**

Case No. 23-SW-2120-DPR

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jeremy Bluto, a Special Agent (SA) with the Homeland Security Investigations, Immigration and Customs Office (HSI / ICE), being first duly sworn, hereby depose and state as follows:

1. I am a SA with Immigration and Customs Enforcement / Homeland Security Investigations, Kansas City, Missouri, Principal Field Office, and have been so employed since April 25, 2010. I am currently assigned as a criminal investigator for HSI. Prior to my current position, I was employed with U.S. Customs and Border Protection, Office of Border Patrol, as a Border Patrol Agent and a Supervisory Border Patrol agent for five years, and a Deputy Sheriff with the Taney County, Missouri, Sheriff's Department for three years. Prior to my employment in Missouri, I attended California State University, Fullerton, and received a bachelor's degree in criminal justice.

2. As part of this affiant's duties with HSI, I investigate criminal violations relating to the production, receipt, possession, and distribution of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have received training in the areas of child pornography, child exploitation, coercion and enticement, and human/sex trafficking.

3. The statements in this affidavit are based on my personal observations, training and experience, investigation of this matter, and information obtained from other agents and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, this affiant has not included each and every fact known to me concerning this investigation. This affiant has set forth the facts necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, are located within the Dropbox account with the screen / user name **Sam Smith**, Dropbox ID: **2703411392**, and the email address of **sstevie625@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., headquartered at 185 Berry Street, 4th Floor, San Francisco, California 94107, also within the Northern District of California, hereinafter referred to as "premises," and further described in Attachment A hereto.

4. This affidavit is in support of an application for a search warrant for evidence, fruits, and instrumentalities of the foregoing criminal violations, which relate to the knowing possession, receipt, distribution, and/or production of child pornography. This affiant requests the authority to search and/or examine the seized items, specified in Attachment B, as instrumentalities, fruits, and evidence of crime.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of 18 U.S.C. §§ 2251, 2252, and 2252A, relating to material involving the production, receipt, possession, and/or distribution of child pornography:

a. 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing, or coercing a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce, or if such visual depiction actually was transported in or affecting interstate commerce.

b. 18 U.S.C. § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

c. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

7. The following definitions apply to this Affidavit and its Attachments:

a. The term “minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term “sexually explicit conduct,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

c. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

d. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

e. The term “child pornography,” as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or

other means, of sexually explicit conduct, where:

- i. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
- ii. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
- iii. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

f. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, and painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to, phonograph records, printing, and typing) or electrical, electronic, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

g. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the

Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

h. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

i. “Domain names” are common, easy to remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

j. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transfer Protocol (HTTP).

DROPBOX INC.

8. “Dropbox” refers to an online storage medium on the internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said

files on their own computer or other electronic storage device. Dropbox is an “offsite” storage medium for data that can be viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual’s computer that utilizes Dropbox would not be able to view these files if the user opted only to store them at an offsite such as Dropbox. These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

9. Dropbox provides a variety of on-line services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

10. When the subscriber transfers a file to a Dropbox account, it is initiated at the user’s computer, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

11. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address (“IP address”) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

12. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well records of any actions taken by the provider or user as a result of the communications.

BACKGROUND OF THE INVESTIGATION

13. On April 24, 2023, I was assigned National Center for Missing and Exploited Children (NCMEC) CyberTipline Report (CTR) 160563517 for investigation as part of my duties as a member of the Southwest Missouri Cybercrime Task Force (SMCCTF).

14. According to CTR 160563517, Dropbox, Inc. discovered a file believed to contain child sexual abuse material (CSAM), otherwise known as child pornography, on or about April

17, 2023. The CTR indicated Dropbox, Inc. had viewed the entire contents of the file and had categorized it as A1, meaning they believed it depicted a sex act involving a prepubescent minor.

15. Dropbox, Inc. provided the following details pertaining to the account holder who uploaded the suspected file:

- i. Email Address: **sstevie625@gmail.com** (Verified 11-17-2019)
- ii. Screen / User Name: **Sam Smith**
- iii. ESP User ID: **2703411392**
- iv. IP Address: 2600:100a:b1c8:2add:753c:b815:80f8:27a6 (Login) 10-31-2022

16. I reviewed the file of suspected CSAM that Dropbox submitted with the CTR. The filename was 2016-12-11 21.32.30.mov, and had a MD5 hash value of 1d29b4b620b0e9103b9dd7eb0d5c1da5. The file was a video file approximately seven seconds in length. The video depicted a nude prepubescent male, who appeared to be no older than six years old. A female, who appeared to be less than 18 years old, was performing oral sex on the male. The video was zoomed in and only the male's stomach, penis, and upper legs were visible, and only the female's head and profile of her face was visible.

17. IP Address 2600:100a:b1c8:2add:753c:b815:80f8:27a6 was registered to Verizon Business.

18. On April 28, 2023, a DHS Summons was served on Verizon Business requesting all account holder information for IP Address 2600:100a:b1c8:2add:753c:b815:80f8:27a6 on October 31, 2022 at 12:44:57 UTC.

19. On May 7, 2023, Verizon business provided a response and indicated the target IP address at the stated date and time was associated with Verizon phone number (417) 236-1976 and provided the following customer information:

- i. Account Number: 589590294-1
- ii. Customer Last Name: SANCHEZ
- iii. Customer First Name: Steven
- iv. Address: 314 Hill Dr.
- v. City: Galena
- vi. State: MO
- vii. Zip Code: 65656

20. A search of the Missouri Department of Revenue database revealed a driver license record for Steven Vincent SANCHEZ, date of birth of May 30, 1969, with residential address of 314 Hill Drive, Galena, Stone County, Missouri 65616, also within the Western District of Missouri.

21. A search of the Missouri Sex Offender Registry revealed that SANCHEZ is a registered sex offender. He is required to register as a sex offender because, on or about February 8, 2011, SANCHEZ was convicted of statutory sodomy in the second degree in the Circuit Court of Greene County, Missouri. This affiant checked the Missouri Sex Offender Registry website on July 28, 2023, and found that SANCHEZ's home address was listed 314 Hill Drive, Galena, Missouri 65616.

22. On August 7, 2023, a federal search warrant was served at 314 Hill Dr., Galena, Missouri. During a post-*Miranda* interview of SANCHEZ, he stated he had Dropbox account

that he can no longer log into, and the email address most likely associated with the account was sstevie625@gmail.com.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

23. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

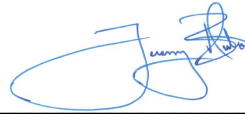
24. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations, or attempted violations, of 18 U.S.C. §§ 2251, 2252, and 2252A, may be located in the Subject Account described in Attachment A.

25. Based on the forgoing, I request that the Court issue the proposed search warrant.

26. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

27. The government will execute this warrant by serving the warrant on Dropbox. Because the warrant will be served on Dropbox, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Further Affiant Sayeth Naught.



JEREMY BLUTO
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me via telephone on the 13th day of September, 2023.



HONORABLE DAVID P. RUSH
Chief United States Magistrate Judge
Western District of Missouri